

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

UNITED STATES OF AMERICA
Plaintiff,

v.

793,510.506954 USDT
Defendant.

§
§
§
§
§
§
§

NO: 6:25-CV-00246

AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE

I, Ian Hetrick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States, Department of Justice, Federal Bureau of Investigation (FBI). I have been assigned to the FBI, Dallas Division, Tyler Resident agency since September 2020. As a Special Agent, my responsibilities include enforcing federal laws as set forth in the United States Code, including those referenced in this application. I have conducted and led numerous investigations of criminal enterprises and individual criminal activity for acts in violation of state and federal statutes and have utilized various investigative techniques. I have also received formal and informal training from the FBI and other organizations on investigation techniques, computer technology, and cybercrime tactics. I have participated in the execution of warrants involving the search and seizure of computers and electronically stored information.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, analysts, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause

for the requested forfeiture. It does not set forth all my knowledge, or the knowledge of others, about this matter.

PROPERTY FOR FORFEITURE

3. This Affidavit is made in support of a civil forfeiture complaint concerning the following personal property:

793,510.506954 USDT seized from Tether deposit addresses 0xbeB0036BC0939D805bB9fCFEc704aF3Cb7C29Ba5 (“0xbeB00”) and 0xDD8A10Df4c86a3584D3ef970BbCD85391c8117Ab (“0xDD8A1”) on or about April 4, 2025 pursuant to a seizure warrant approved by a United States Magistrate Judge for the Eastern District of Texas in Case No. 6:24-MJ-289 (the “Defendant Property”).

LEGAL AUTHORITY FOR FORFEITURE

4. Based on my training and experience and the facts as set forth in this affidavit, the funds to be forfeited represent proceeds of a fraudulent cryptocurrency investment scheme. I believe these funds are proceeds derived from violations of 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud), and 18 U.S.C. § 1343 (Wire Fraud) and were involved in violations of 18 U.S.C. § 1956(h) (Conspiracy to Commit Money Laundering), 18 U.S.C. § 1956 (Money Laundering).

5. 18 U.S.C. § 1343 (Wire Fraud) prohibits, in pertinent part, whoever, having devised to intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, from transmitting or causing to be transmitted by means of wire, radio or television communication in interstate or foreign commerce, any writings, signs, signals, pictures or

sounds for the purpose of executing such scheme or artifice. 18 U.S.C. § 1349 prohibits conspiring to commit wire fraud in violation of 18 U.S.C. § 1343.

6. 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) prohibits, in pertinent part, whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such financial transaction which in fact involves the proceeds of specified unlawful activity knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity. 18 U.S.C. § 1956(h) prohibits conspiring to commit money laundering.

7. I believe the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C). Under 18 U.S.C. § 981(a)(1)(A), “[a]ny property, real or personal, involved in a transaction or attempted transaction” in violation of 18 U.S.C. §§ 1956 or 1957 or “any property traceable to such property” is subject to forfeiture to the United States. Under 18 U.S.C. § 981(a)(1)(C), “[a]ny property, real or personal, which represents or is traceable to the gross receipts obtained, directly or indirectly, from a violation of” “any offense constituting ‘specified unlawful activity,’ or a conspiracy to commit such offense” is subject to forfeiture to the United States.¹

¹ Title 18, United States Code, Section 1343 is a “specified unlawful activity” pursuant to 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1).

8. Property subject to civil forfeiture under 18 U.S.C. § 981(a)(1) may be seized pursuant to 18 U.S.C. § 981(b). Property subject to criminal forfeiture under 18 U.S.C. § 982(a)(1) may be seized pursuant to 21 U.S.C. § 853(f) (by 18 U.S.C. § 982(b)(1)).

DEFINITIONS AND BACKGROUND

TECHNICAL BACKGROUND CONCERNING THE CRIMINAL CONDUCT

9. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

10. A domain name is a simple, easy-to-remember way for humans to identify computers on the internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, “usdoj.gov” and “cnn.com” are domain names.

11. The term “spoofed” refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to persuade consumers that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal.

12. The term “shell company” describes businesses that exists primarily as a means to conduct financial maneuvers and which typically have no employees, provide no actual business or service, and offer some anonymity to the beneficial owners. Criminal entities use shell companies to establish business bank accounts so that large sums of monies can be transacted with less potential suspicion from financial institutions. Bank accounts belonging to shell companies are frequently closed by financial

institutions because of fraud reports made by victims. As a result, shell companies are often used to open accounts at different financial institutions.

BACKGROUND ON VIRTUAL CURRENCY

13. **Virtual Currency:** Virtual currencies are digital tokens of value circulated over the Internet. Virtual currencies are typically not issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Different virtual currencies operate on different blockchains, and there are many different, widely used virtual currencies currently in circulation. Bitcoin (or BTC) and Ether (ETH) are currently the most well-known virtual currencies in use. BTC exists on the Bitcoin blockchain, and ETH exists on the Ethereum network. Typically, a virtual currency that is “native” to a particular blockchain cannot be used on a different blockchain. Thus, absent technological solutions, those native assets are siloed within a specific blockchain. For instance, ETH (the native token on the Ethereum network) cannot be used on other networks unless it is “wrapped” by smart contract code. This wrapping process results in what is called Wrapped ETH or WETH.

14. **Stablecoins:** Stablecoins are a type of virtual currency whose value is pegged to a commodity’s price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. Stablecoins achieve their price stability via collateralizations (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

15. **Tether (USDT):** Tether Limited (“Tether”) is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT, a stablecoin

pegged to the U.S. dollar. Unlike other cryptocurrencies such as Bitcoin whose price tends to fluctuate more unpredictably, Tether tries to hold its value around a specific asset. As a stablecoin, it is pegged or “tethered” to the U.S. dollar as the coin’s name suggests in order to minimize price volatility. Payments or transfers of value made with Tether are recorded on blockchains and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire Tether through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), cryptocurrency ATMs, or directly from other people. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Tether transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous. And while it is not completely anonymous, Tether allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

16. **Virtual Currency Address:** Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency

address is analogous to a bank account number and is represented as a string of letters and numbers.

17. **Private Key:** Each virtual currency address is controlled using a unique corresponding private key, a cryptographic equivalent of a password, which is needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

18. **Virtual Currency Wallet:** Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–63 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

19. There are various types of virtual currency wallets, including software wallets, hardware wallets, and paper wallets. The virtual currency wallets at issue for the purposes of this affidavit are software wallets (*i.e.*, a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses

and private keys). A virtual currency wallet allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time.

20. Wallets that are hosted by third parties are referred to as “hosted wallets” because the third party retains a customer’s funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are often called “unhosted” wallets.

21. Although cryptocurrencies have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement’s efforts to track transactions.

22. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device (“hardware wallet”), downloaded on a PC or laptop (“desktop wallet”), with an Internet-based cloud storage provider (“online wallet”), as a mobile application on a smartphone or tablet (“mobile wallet”), printed public and private keys (“paper wallet”), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or

removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (*e.g.*, Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code² with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a “recovery seed” (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

23. **Blockchain:** Many virtual currencies publicly record all their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain’s technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

² A QR code is a matrix barcode that is a machine-readable optical label.

24. **Blockchain Explorer:** These explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses API³ and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format.

25. **Smart Contracts:** Smart contracts are computer programs stored on a blockchain that run when predetermined conditions are met. Typically, they are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement. The Ethereum network is designed, and functions based on smart contracts.

26. **Virtual Currency Bridge:** A blockchain bridge, otherwise known as a cross-chain bridge, connects two blockchains and allows users to send virtual currency from one chain to the other.

27. **Virtual Currency Exchanges (VCEs):** VCEs are trading and/or storage platforms for virtual currencies, such as BTC and ETH. There are generally two types of VCEs: centralized exchanges and decentralized exchanges, which are also known as "DEXs." Many VCEs also store their customers' virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses associated with a user on a VCE's network. Because VCEs act as money services

³ API is an initialism for "application programming interface," which is a set of definitions and protocols for building and integrating application software.

businesses, they are legally required to conduct due diligence of their customers (*i.e.*, KYC checks) and to have anti-money laundering programs in place (to the extent they operate and service customers in the United States).

28. **Instant VCEs:** Instant exchanges allow their customers to swap (*i.e.*, exchange) one virtual currency for another. Instant exchanges typically do not act as a custodian of their customers' assets in the way that larger VCEs do. In other words, a customer would not store his or her virtual currency on an Instant VCE's platform; instead, he or she would conduct trades and then either move funds to a third-party VCE that acts as a custodian (*i.e.*, a hosted wallet) or move funds to his or her unhosted wallet.

29. **Virtual Currency Mixers:** Virtual currency mixers (also known as tumblers or mixing services) are software services that allow users, for a fee, to send virtual currency to designated recipients in a manner designed to conceal and obfuscate the source of the virtual currency. Based on my training and experience, I know that virtual currency mixers are a common laundering tool used by criminal cyber actors and their money laundering co-conspirators.

30. **Blockchain Analysis:** As previously stated, while the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain (*e.g.*, the Bitcoin blockchain). The analysis can also reveal additional addresses controlled by the same individual or entity. "For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (*i.e.*, a "cluster"). It is possible to identify a 'cluster' of [BTC] addresses held by

one organization by analyzing the [BTC] blockchain's transaction history. Open-source tools and private software products can be used to analyze a transaction." *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020).

31. Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement officers use reputable, free open-source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to be reliable.

32. In addition to using publicly available blockchain explorers, law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

33. **Decentralized Finance (DeFi):** Decentralized Finance, or DeFi, is an umbrella term for financial services on public blockchains, primarily the Ethereum network. The Ethereum network's native virtual currency is ETH. Ethereum was the first blockchain that offered various decentralized services within its network. To make these

services possible, the Ethereum network allows other tokens besides ETH to run within the network. These tokens are known as ERC-20 tokens.

34. DeFi is a term used to describe a financial system that operates without the need for traditional, centralized intermediaries. Instead, DeFi platforms offer an alternative financial system that is open for anyone to use, and that allows centralized intermediaries to be replaced by decentralized applications (or dApps). With DeFi, one can do most of the things that banks support—earn interest, borrow, lend, buy insurance, trade derivatives, trade assets, etc.—but it is faster than using traditional banks and does not require paperwork or a third party. DeFi is global, peer-to-peer (*i.e.*, directly between two people rather than routed through a centralized system), pseudonymous, and open to the public.

FACTS SUPPORTING FORFEITURE

35. The United States is investigating a fraud and money laundering scheme. The investigation concerns possible violations of, inter alia, 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud), 18 U.S.C. § 1956 (Money Laundering), and 18 U.S.C. § 1956(h) (Conspiracy to Commit Money Laundering). This investigation has revealed that the Defendant Property consists of proceeds from various wire fraud schemes within the United States, including within the Tyler Division of the Eastern District of Texas.

36. In February 2023, FBI Dallas began an investigation of a criminal money laundering syndicate operating cryptocurrency investment scams. In particular, the unknown scammers promoted spoofed domains and websites purporting to look like

legitimate cryptocurrency trading platforms to U.S.-based victims, including victims located in Tyler, Texas, which is within the Eastern District of Texas. Scammers then fooled victims into “investing” in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal the victims’ money.

37. This type of scam is often identified as “pig butchering” (derived from the Chinese phrase used to describe this scheme) and involves scammers spending significant time getting to know, targeting, and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. The victims are then typically asked to invest their funds through a provided cryptocurrency (BTC, USDT, ETH, or USDC) deposit address and are further told they can expect to make a sizeable return on their investments. As initial smaller investments are made, the spoofed websites falsely display a significant increase in the victim’s account balance, which entices the victim to continue making investments, which typically end with a final large deposit or transaction. When the victim attempts to make a withdrawal, the scammers attempt to coerce the victims to make additional investments. These tactics can include requesting additional investments due to “significant profits” gained on the account or other reasons such as freezing the account due to “taxes owed” or “suspicious behavior.” Regardless of how the scammers attempt to solicit additional investments from the victims, the victims are unable to retrieve any portion of their investment.

38. On or about February 22, 2023, FBI Dallas received a call from L.H. in Tyler, Texas that she believed she may have been a victim of an illegal investment scheme.

39. On or about October 25, 2022, L.H. received an email from Mica F. Tan (Micatanmft0813@gmail.com), who purported to be interested in buying property. Tan also presented herself as an expert in cryptocurrency trading. After developing a business relationship, Tan taught L.H. to trade cryptocurrency. In or around November 16, 2022 and February 9, 2023, after receiving assurances of the safety of the website for investments and developing trust in Tan, L.H. and four partners (L.H.) agreed to invest in cryptocurrency through <https://hopexaub.com/#/home>. L.H. began to send cryptocurrency to hopexaub.com's wallet address 0x250aF2175F030566DbA21455Dbc97D64B7Ecd921 (0x250aF2) as detailed in the table below. L.H. believed <https://hopexaub.com/> was a legitimate website for trading cryptocurrency. The platform appeared authentic and had customer service lines that could be contacted.

Date	Amount	Hopexaub.com Wallet
November 16, 2022	\$95,000.00	0x250aF2175F030566DbA21455Dbc97D64B7Ecd921
November 23, 2022	\$134,100.00	0x250aF2175F030566DbA21455Dbc97D64B7Ecd921
December 20, 2022	\$169,000.00	0x250aF2175F030566DbA21455Dbc97D64B7Ecd921
December 21, 2022	\$31,000.00	0x250aF2175F030566DbA21455Dbc97D64B7Ecd921
January 9, 2024	\$105,000.00	0x250aF2175F030566DbA21455Dbc97D64B7Ecd921
January 20, 2024	\$75,000.828	0x250aF2175F030566DbA21455Dbc97D64B7Ecd921
January 27, 2024	\$25,000.00	0x250aF2175F030566DbA21455Dbc97D64B7Ecd921
January 27, 2024	\$100,000.00	0x250aF2175F030566DbA21455Dbc97D64B7Ecd921
February 1, 2024	\$75,000.00	0x250aF2175F030566DbA21455Dbc97D64B7Ecd921

40. When L.H. tried to withdraw funds from L.H.'s cryptocurrency account at hopexaub.com, the trading platform required L.H. to send a 5% fee (on top of the initial cryptocurrency deposits) to "verify" that L.H. was not laundering money. L.H. then

contacted Tan via WhatsApp and told Tan that she could not pay 5%. Tan instructed L.H. to pay what she could, and Tan would cover the rest. At this point, L.H. believed she was the victim of a scam.

41. All of L.H.'s cryptocurrency transactions were traced to the Subject Tether (USDT) addresses, as detailed below. The traces were conducted using the Last-In, First-Out accounting principle – meaning the most recently deposited items are recorded as the next withdrawal. For clarity, all cryptocurrency addresses have been shortened to the first eight characters.

Tracing of Victim Funds to the Subject USDT Addresses

42. Prior to reporting the loss to the FBI on February 22, 2023, L.H. contracted with a private company to conduct a Blockchain analysis investigation into the movement of cryptocurrency funds. The company provided an initial report on February 20, 2023, and a subsequent report on March 23, 2023. The FBI Virtual Currency Response Team (VCRT) recreated the private company's analysis and confirmed the findings.

43. In nine transactions, L.H. transferred cryptocurrency from her wallet at crypto.com to the hopexaub.com website wallet at 0x250aF2, for \$809,100.828 USDC of cryptocurrency, worth \$809,100.828 USD. The transactions included the following:

Date	Time	Amount	Transaction Hash
November 16, 2022	16:17 UTC	94,900 USDC	Oxeef8a9a468daa7b19b2e5af6a6e72635705376cb25679f9b8db7a268472b9b2f
November 23, 2022	18:19 UTC	134,090 USDC	Ox72054378dc709c0d849875e2233fbcf9baaa27bda6blf43847607514cefcbb2
December 20, 2022	16:12 UTC	168,990 USDC	Ox3b7490eaf197ebcb7f4350ebba4dab5ca0975dlfcb9f521b879e73113b7ab3e

December 21, 2022	16:21 UTC	30,990 USDC	Oxacf025c4953ec9ac33769eb48a4lbea9f8fdcf4a57a0a5c7e4beebfd1874b5cc
January 20, 2023	18:10 UTC	74,990 USDC	Oxe4afdc608bc2e5cacb27c436db1e3d71f330cdf5051a3d9d3d8ae5dc935a60d3
January 27, 2023	16:52 UTC	24,990 USDC	Ox5578a4bl861557ad34ec82aba448bb07ca70641c7155b7e8292447b34b598b01
January 27, 2023	20:00 UTC	99,990 USDC	Ox8930345cb59769fa3b27668a719f9630d998fb5060a176b3edeafadef0994a
February 1, 2023	15:54 UTC	74,990 USDC	Ox0b555768a7e87c561525235bf28076e349023laaa9f666e28648c03cfe2fb3c0
February 9, 2023	16:44 UTC	104,990 USDC	Oxb39c64e30cefb93a54b0eb46a3975294be68f8e6d9d4d26246bd8794b6320724

44. Within wallet 0x250aF2, L.H.'s funds were then commingled with additional USDC. These funds were transferred out between on or about November 16, 2022, and February 09, 2023 in nine separate transactions totaling 809,010 USDC to consolidation wallet address 0x1939e198E608A4e84466ff918Ba728c30281f1f8 (0x1939e1). Through a series of transactions occurring between on or about December 14, 2022 and April 24, 2023, the funds were converted from USDC to Ether to DAI in wallets 0x3BE6e561D5814f9e02F28Cca179026c43C79fEa3 (0x3BE6e5) and 0xA5DAC7B604324dd16a90Fa199389e68830b3b2bc (0xA5DAC7). Within wallets 0x3BE6e5 and 0xA5DAC7, L.H.'s funds were commingled with additional cryptocurrency.

Date	Origin Wallet	Destination Wallet	Amount	Transaction Hash
December 14, 2022	0x1939e1	0x3BE6e5	61,866 DAI	0x45ea1ffa45bc8dba4a567b351ee92223c245eb8ab809afc4bc54f6a2cb7c5e12
December 20, 2022	0x1939e1	0x3BE6e5	168,902 DAI	0xc9520f5df7fb3d24a39d742504630d2ba77d1815a3c454083f558ddf8194a2ea
December 23, 2022	0x1939e1	0x3BE6e5	45,845 DAI	0xfeae642c810e398d804508e5a7e9c5125859f8326b3513b71a76c60d48a37513
January 20, 2023	0x1939e1	0x3BE6e5	85,273.9 DAI	0x7df4f57781b427a6f74f544a8f34228afb6e08822538a97f31cabddf883b8c1d
January 27, 2023	0x1939e1	0x3BE6e5	131,500 DAI	0x66f6e4009d613b9880507d13b2f661d2a62a2ca4a93d7b0724684b2e0e140424
April 24, 2023	0x1939e1	0xA5DAC7	0.10 ETH	0x3d2451e0cbf59a308c0586a3b3f65eef55c1bf523b5c809892f50ae4d0411675

45. On or about December 13, 2022 and January 27, 2023, in multiple transactions, wallet 0xA5DAC7 sent \$1,337,032 DAI to wallet 0x3BE6e5. On or about January 31, 2023 and April 6, 2023, in multiple transactions, wallet 0xA5DAC7 sent \$1,062,560 DAI and 39,328 USDT to wallet 0x6C4cBEa1863b252F6cD2A987e0D0cb8882a0f8e4 (0x6C4cBE). Within wallet 0x6C4cBE, L.H.'s funds were commingled with additional cryptocurrency.

Date	Origin Wallet	Destination Wallet	Total Amount
December 13, 2022	0xA5DAC7	0x3BE6e5	
January 27, 2023	0xA5DAC7	0x3BE6e5	\$1,337,032 DAI
Date	Origin Wallet	Destination Wallet	Total Amount
January 31, 2023	0xA5DAC7	0x6C4cBE	
April 6, 2023	0xA5DAC7	0x6C4cBE	\$1,062,560 DAI and 39,328 USDT

46. On March 25, 2023, the private company that L.H. had hired contacted the FBI to report how it had identified four wallets owned by Tether that included funds from L.H. and which were identified through analysis of incoming funds as belonging to the fraud ring.

47. On March 27, 2023, FBI emailed a request to Tether to freeze the identified wallets. On April 5, 2023, Tether responded to the March 27, 2023 request to freeze wallets and stated that funds had been moved from the wallets. Tether identified three wallets that could be frozen based on their analysis of the movement of funds.

48. On April 5, 2023, the private company reviewed information provided by Tether and confirmed the link of funds initially deposited by L.H. and the wallets identified by Tether.

49. On April 7, 2023, Tether confirmed the freezing of the following accounts, including the two accounts comprising the Defendant Property:

Frozen Account	Wallet Addresses	Balance as of June 18, 2024
1 (0xbeB00)	0xbeB0036BC0939D805bB9fCFEc704aF3Cb7C29Ba5	683,652 USDT
2 (0xDD8A1)	0xDD8A10Df4c86a3584D3ef970BbCD85391c8117Ab	232,023 USDT
3 (0x32854)	0x32854585d620b74733430796D5A5DdD4085E3c10	232,072.93 USDT
4 (0x23fc7)	0x23fc72Be7f0e751B2C6C8eC7d347f69Dab630504	33,106.41 USDT

50. FBI VCRT conducted blockchain analysis and identified wallets 0x1939e1, 0xA5DAC7, and 0x6C4cBE that transferred commingled funds, to include L.H.'s funds.

The following chart identifies movement of L.H.'s funds from consolidation wallets:

Origin Wallet	Destination Wallet	Date	Amount
Frozen Account 2 (0xDD8A1)	0x1939e1	January 23, 2023 to February 09, 2023	\$0.15 ETH
Origin Wallet	Destination Wallet	Date	Amount
0xA5DAC7	0x6C4cBE	January 31, 2023 to April 6, 2023	\$ 1,062,560 DAI and 39,328 USDT
0xA5DAC7	0x9c049501A942Af7f20375AEb438490EC9D280F9 (0x9c0495)	April 2, 2023	\$ 0.20 ETH
0x9c0495	0x0077Ae58494c215D70FDCf242E4931079619742f (0x0077Ae)	April 2, 2023	\$ 0.09 ETH
0x0077Ae	Frozen Account 1 (0xbeB00)	April 2, 2023	\$84,965 USDT
Origin Wallet	Destination Wallet	Date	Amount
0x6C4cBE	Frozen Account 4 (0x23fc7)	April 6, 2023	\$877,326 DAI
0x6C4cBE	Frozen Account 3 (0x32854)	April 6, 2023	\$703,327 DAI

51. On or about September 3, 2024, the United States Attorney's Office for the Eastern District of Arkansas served a seizure warrant on Tether for two of the four frozen accounts.

Frozen Account	Wallet Addresses	Balance as of June 18, 2024
3 (0x32854)	0x32854585d620b74733430796D5A5DdD4085E3c10	232,072.93 USDT
4 (0x23fc7)	0x23fc72Be7f0e751B2C6C8eC7d347f69Dab630504	33,106.41 USDT

52. FBI Little Rock received the USDT for Tether wallets 0x32854 and 0x23fc7 and has initiated administrative forfeiture procedures.

53. With respect to Tether wallets 0xbeB00 and 0xDD8A1, a total of 793,510.506954 in USDT was seized pursuant to a seizure warrant on or about April 4, 2025.

CONCLUSION

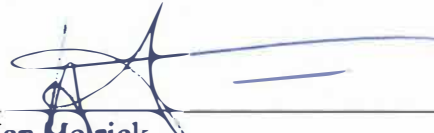
54. I submit that this affidavit supports probable cause to forfeit all funds, monies, and other things of value up to 793,510.506954 USDT seized from Tether deposit addresses 0xbeB0036BC0939D805bB9fCFEc704aF3Cb7C29Ba5 and 0xDD8A10Df4c86a3584D3ef970BbCD85391c8117Ab on or about April 4, 2025.

55. Based on my experience and the information herein, I have probable cause to believe that the seized 793,510.506954 USDT constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)), are traceable to a money laundering transaction and are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

56. I also have probable cause to believe that the seized 793,510.506954 USDT constitutes proceeds traceable to a violation of 18 U.S.C. § 1343 and/or 18 U.S.C. § 1349, and are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

As provided in 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Respectfully submitted,

A handwritten signature in blue ink, appearing to read "Ian Helrick", is written over a horizontal line.

Ian Helrick
Special Agent
Federal Bureau of Investigation